

**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ**

**Харківський національний університет внутрішніх справ**

**Кафедра кібербезпеки та DATA-технологій, факультет №6**

## **РОБОЧА ПРОГРАМА**

навчальної дисципліни «**Стандартизація і сертифікація в галузі  
інформаційної безпеки**»

обов'язкових компонент освітньої програми  
другого магістрського рівня вищої освіти

Спеціальність: 125 Кібербезпека ( безпека інформаційних та комунікаційних  
систем)

**Харків 2023 р.**

## **ЗАТВЕРДЖЕНО**

Науково-методичною радою  
Харківського національного  
університету внутрішніх справ  
Протокол від 30 .01.23 № 1

## **СХВАЛЕНО**

Вченою радою факультету № 6  
Протокол від 13 .01.23 № 1

## **ПОГОДЖЕНО**

Секцією Науково-методичної ради  
ХНУВС з технічних дисциплін  
Протокол від 27 .01.23 № 1

Розглянуто на засіданні кафедри кібербезпеки та DATA-технологій  
(протокол від 13 .01.23 № 1)

### **Розробники:**

1. Професор кафедри, д.т.н., професор Можєєв О.О.
2. Професор кафедри, д.т.н., професор Семенов С.Г.
3. Доцент кафедри, д.т.н., Можєєв М.О.

### **Рецензенти:**

1. Доцент кафедри боротьби з кіберзлочинністю ХНУВС, к.т.н., доцент Клімушин П.С.;
2. Завідувач кафедри ЕОМ ХНУРЕ д.т.н., професор, Коваленко А.А.

## 1. Опис навчальної дисципліни

Найменування показників	Шифри та назви галузі знань, код та назва спеціальності, ступень вищої освіти	Характеристика навчальної дисципліни
Кількість кредитів ECTS – 6 Загальна кількість годин – 180 Кількість тем – 5	<u>12</u> <u>Інформаційні технології</u> ; <small>(шифр галузі) (назва галузі знань)</small> <u>125 – Кібербезпека</u>  <u>магістр</u> <small>(назва СВО)</small>	Цикл дисциплін професійної та практичної підготовки Навчальний курс –1 Семестр –2 Види контролю: екзамен
Тижневих годин для денної форми навчання: аудиторних – 2,5 самостійної роботи – 4,5		Розподіл навчальної дисципліни за видами занять: (денна форма навчання) Лекції – 30; Практичні заняття – 30; Самостійна робота – 120; (заочна форма навчання) Лекції – 6; Практичні заняття – 10; Самостійна робота – 164; Індивідуальні завдання:

## 2. Мета та завдання навчальної дисципліни

**Мета** викладання навчальної дисципліни «Стандартизація і сертифікація в галузі інформаційної безпеки» є вивченні наукових, методичних та організаційних основ діяльності міжнародних і регіональних систем стандартизації і сертифікації (підтвердження відповідності) систем захисту інформації.

**Основними завданнями** вивчення дисципліни „Стандартизація і сертифікація в галузі інформаційної безпеки ” є надання даних та вивчення студентами основних регламентаційних документів щодо стандартизації та сертифікації.

**Міждисциплінарні зв'язки:** викладання дисципліни «Стандартизація і сертифікація в галузі інформаційної безпеки» базується на знаннях дисциплін «Основи захисту інформації», «Інформаційні технології», «Електроніка та схемотехніка».

**Очікувані результати навчання:** у результаті вивчення навчальної дисципліни здобувач вищої освіти повинен:

**знати:**

- правові основи стандартизації і сертифікації;
- основні поняття і визначення стандартизації та сертифікації в галузі інформаційної безпеки;
- основні положення систем (комплексів) загальнотехнічних і організаційно-методичних стандартів в галузі інформаційної безпеки;
- показники якості і методи їх оцінки;
- системи якості в галузі інформаційної безпеки;
- основні терміни та визначення в галузі сертифікації в галузі інформаційної безпеки;
- організаційну структуру сертифікації в галузі інформаційної безпеки;
- системи і схеми сертифікації в галузі інформаційної безпеки;
- основи стандартизації інформаційного та програмного забезпечення;

**вміти:**

- надавати мережеві послуги за допомогою призначених для користувача програм;
- застосовувати вимоги нормативних документів до основним видам продукції (послуг) і процесів;
- застосовувати документацію систем якості;
- застосовувати основні правила і документи системи сертифікації.

**мати уяву про:**

- перспективи і тенденції розвитку сучасних методологій стандартизації і сертифікації в галузі інформаційної безпеки;
- можливості сучасних технічних засобів перевірки відповідності;
- можливості та перспективи використання засобів перевірки відповідності у своїй роботі за спеціальністю.

В навчальному плані для вивчення дисципліни передбачені такі організаційні форми занять як лекції і практичні і лабораторні заняття.

<b>Програмні компетентності, які формуються при вивченні навчальної дисципліни:</b>		
<b>Інтегральна компетентність</b>	Здатність самостійно досліджувати і розроблювати комплексні системи забезпечення кібербезпеки, викладати і здійснювати аналітичну діяльність в області кібербезпеки.	
<b>Загальні компетентності (ЗК)</b>	ЗК-1	Здатність до абстрактного, логічного, критичного мислення та встановлення взаємозв'язків між явищами та процесами.
	ЗК-2	Здатність приймати управлінські й обґрунтовані рішення в складних і непередбачуваних умовах
	ЗК-3	Здатність удосконалювати й розвивати свій інтелектуальний і загальнокультурний

		рівень, уміння набувати нові знання, використовуючи сучасні інформаційні технології
	ЗК-6	Набуття гнучкого способу мислення, який дає можливість зрозуміти й розв'язати проблеми та задачі, зберігаючи при цьому критичне відношення до усталених наукових концепцій
	ЗК-7	Здатність провести усну презентацію та написати зрозумілу статтю за результатами проведених досліджень, а також щодо сучасних загроз і концепцій у забезпечення кібербезпеки для загальної публіки (не фахівців)
	ЗК-8	Досягнення необхідних знань і розуміння ролі кібербезпеки для інформаційного суспільства з метою адекватної роботи за майбутніми професіями та врахування впливу на соціальні проблеми
<b>Спеціальні (фахові, предметні) компетентності (СК)</b>	ФК-2	Здатність формулювати, аналізувати та синтезувати рішення наукових проблем на абстрактному рівні шляхом декомпозиції їх на складові, які можна дослідити окремо в їх більш та менш важливих аспектах
	ФК-3	Здатність будувати відповідні моделі сценаріїв кіберризиків, досліджувати їх для отримання нових висновків та поглиблення розуміння природи кіберзагроз
	ФК-4	Здатність розробляти і впроваджувати комп'ютерні програми та використовувати існуючі
	ФК-5	Здатність комунікувати з колегами з даної області щодо наукових досягнень, як на загальному рівні, так і на рівні спеціалістів, здатність робити усні та письмові звіти, обговорювати наукові теми рідною та англійською мовами

### 3. Програма навчальної дисципліни

#### ТЕМА № 1. Сутність стандартизації.

Місце, роль та задачі дисципліни. Предмет, структура і зміст дисципліни. Поняття стандарту. Види стандартизації. Міжнародна стандартизація.

## **ТЕМА № 2. Нормативно-правове забезпечення з питань стандартизації.**

Нормативно-правове забезпечення з питань стандартизації. Закони України “Про стандартизацію”, „Про технічні регламенти та оцінку відповідності”, “Про телекомунікації”, “Про радіочастотний ресурс України”.

## **ТЕМА № 3. Управління ризиками інформаційної безпеки.**

Підходи до управління ризиками інформаційної безпеки. Вимоги стандарту ISO/IEC 27005.

## **ТЕМА № 4. Нормативно-правове забезпечення з питань оцінки відповідності (сертифікації).**

Нормативні документи з технічного захисту інформації України. Критерії оцінки захищеності від НСД та профілі захисту в АС. Практика застосування критеріїв оцінки захищеності інформації в КС від НСД

## **ТЕМА № 5. Оцінювання на відповідність**

Підготовка до оцінювання. Проведення оцінювання. Підтвердження результатів оцінювання.

## **ТЕМА № 6. Методологічне забезпечення питань сертифікації в галузі інформаційної безпеки.**

Аналіз принципів побудови моделей інформаційної безпеки. Методика оцінювання стану захисту інформації локальних об’єктів

## **4. Структура навчальної дисципліни**

### **4.1. Розподіл часу навчальної дисципліни за темами (денна форма навчання)**

Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни					Література, сторінки	Вид контролю
	Всього	з них:					
		лекції	Семінарські заняття	Практичні заняття	Лабораторні заняття		
Семестр 2							
Тема № 1: Сутність стандартизації.	8	4		4		25	1
Тема № 2: Нормативно-правове забезпечення з питань стандартизації.	76	6		6		25	1
Тема № 3: Управління ризиками інформаційної безпеки	36	6		6		26	2
Тема 4. Нормативно-правове забезпечення з питань оцінки відповідності (сертифікації).	38	4		4		18	

Тема 5. Оцінювання на відповідність	46	6		6		22		
Тема 6. Методологічне забезпечення питань сертифікації в галузі інформаційної безпеки	42	4		4		17		
<b>Всього за семестр</b>	<b>210</b>	<b>30</b>		<b>30</b>		<b>105</b>		<b>екзамен</b>

#### 4.2. Розподіл часу навчальної дисципліни за темами (заочна форма навчання)

Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни					Література, сторінки	Вид контролю	
	Всього	з них:						
		лекції	Семінарські заняття	Практичні заняття	Лабораторні заняття			Самостійна робота
Семестр 2								
Тема № 1: Сутність стандартизації.	8	4		4		25	1	
Тема № 2: Нормативно-правове забезпечення з питань стандартизації.	76	6		6		25	1	
Тема № 3: Управління ризиками інформаційної безпеки	36	6		6		26	2	
Тема 4. Нормативно-правове забезпечення з питань оцінки відповідності (сертифікації).	38	4		4		18		
Тема 5. Оцінювання на відповідність	46	6		6		22		
Тема 6. Методологічне забезпечення питань сертифікації в галузі інформаційної безпеки	42	4		4		17		
Всього за семестр	210	30		30		105		екзамен

#### 4.3. Питання, що виносяться на самостійне опрацювання.

Завдання що виносяться на самостійну роботу студента		Література:
	Тема № 1: Сутність стандартизації..	Конспект лекцій, література [1-5]
	Місце, роль та задачі дисципліни. Предмет, структура і зміст дисципліни.	Конспект лекцій, література [1-5]1
	Поняття стандарту. Види стандартизації..	Конспект лекцій, література [1-5]
	Міжнародна стандартизація.	Конспект лекцій,

		література [1-5]
	Тема № 2: Нормативно-правове забезпечення з питань стандартизації.	Конспект лекцій, література [1-9]1
	Нормативно-правове забезпечення з питань стандартизації.	Конспект лекцій, література [1-9]
	Закони України “Про стандартизацію”,	Конспект лекцій, література [1-9]
	Закони України „Про технічні регламенти та оцінку відповідності”	Конспект лекцій, література [1-9]
	Закони України “Про телекомунікації”, “Про радіочастотний ресурс України”.	Конспект лекцій, література [1-9]
	Тема № 3: Управління ризиками інформаційної безпеки.	Конспект лекцій, література [1-9]
	Підходи до управління ризикам інформаційної безпеки.	Конспект лекцій, література [1-9]
	Вимоги стандарту ISO/IEC 27005.	Конспект лекцій, література [1-9]
	Тема № 4: Нормативно-правове забезпечення з питань оцінки відповідності (сертифікації).	література [5-9]
	Нормативні документи з технічного захисту інформації України.	література [1-9]
	Критерії оцінки захищеності від НСД та профілі захисту в АС.	література [1-9]
	Практика застосування критеріїв оцінки захищеності інформації в КС від НСД	література [1-9]
	Тема № 5: Оцінювання на відповідність	література [1-9]
	Підготовка до оцінювання.	література [1-9]]
	Проведення оцінювання.	література [1-9]
	Підтвердження результатів оцінювання.	література [1-9]
	Тема № 6: Методологічне забезпечення питань сертифікації в галузі інформаційної безпеки.	література [1-9]
	Аналіз принципів побудови моделей інформаційної безпеки.	література [1-9]
	Методика оцінювання стану захисту інформації локальних об’єктів.	література [1-9]

## 5. Індивідуальні навчально-дослідні завдання

Не передбачено освітньо-професійною програмою.

## 6. Методи навчання

Вивчення курсу дозволить слухачам оволодіти необхідними теоретичними знаннями щодо побудови та принципів функціонування інформаційних систем. В навчальному плані для вивчення дисципліни передбачені такі організаційні форми занять як лекції та практичні заняття.

На лекційних заняттях викладаються теоретичні засади тем, що вивчаються, а також приклади їх використання для розв’язання конкретних навчальних задач.

На практичних заняттях слухачі відпрацьовують під керівництвом викладача прийоми розв’язання типових задач. Практичні заняття проводяться в комп’ютерному класі. Практичні заняття проводяться у зведеному форматі, що дозволяє більш ефективно використовувати комп’ютерну техніку.

Перед практичним заняттям слухач повинен вивчити певний теоретичний матеріал і (можливо) виконати практичне завдання у відповідності



до методичних вказівок до практичних занять з дисципліни. Після закінчення практичного заняття слухач отримує домашнє завдання для закріплення практичних навичок розв'язання задач.

Основним видом інформаційно-методичного забезпечення дисципліни є:

- конспект лекцій;
- методичні вказівки до практичних занять;
- навчальні посібники з дисципліни.

Перелічені складові елементи інформаційно-методичного забезпечення існують як у друкованому вигляді так і в електронній формі у вигляді роздаткових матеріалів, відповідного розділу сайту кафедри інформаційних систем , а також у вигляді електронного навчального комплексу з дисципліни на компактному диску.

## **7. Перелік питань та завдань, що виносяться на підсумковий контроль**

1. Поняття стандарту. Види стандартизації. Міжнародна стандартизація.
2. Нормативно-правове забезпечення з питань стандартизації.
3. Закони України “Про стандартизацію”.
4. Мета стандартизації та основні принципи державної політики у сфері стандартизації.
5. Об’єкти стандартизації.
6. Суб’єкти стандартизації
7. Основні засади, процедури розроблення і прийняття та застосування національних стандартів, кодексів усталеної практики та змін до них
8. Інформаційне забезпечення та право власності на національні стандарти, кодекси усталеної практики та каталоги і використання коштів, одержаних від їх реалізації
9. Міжнародне співробітництво та фінансування робіт із стандартизації
10. Закони України „Про технічні регламенти та оцінку відповідності”.
11. Повноваження органів виконавчої влади у сфері технічного регулювання
12. Технічні регламенти та процедури оцінки відповідності
13. Особливості розроблення та прийняття технічних регламентів і процедур оцінки відповідності
14. Надання інформації про технічні регламенти, стандарти та процедури оцінки відповідності
15. Закони України “Про телекомунікації”.
16. Закони України “Про радіочастотний ресурс України”.
17. Підходи до управління ризикам інформаційної безпеки.
18. Державні стандарти.
19. Вимоги стандарту ISO/IEC 27005.
20. Нормативні документи з технічного захисту інформації України.
21. Критерії оцінки захищеності від НСД та профілі захисту в АС.
22. Практика застосування критеріїв оцінки захищеності інформації в КС від НСД
23. Підготовка до оцінювання безпеки.
24. Проведення оцінювання безпеки.
25. Підтвердження результатів оцінювання безпеки.
26. Аналіз принципів побудови моделей інформаційної безпеки.
27. Методика оцінювання стану захисту інформації локальних об’єктів.

## 8. Критерії та засоби оцінювання результатів навчання здобувачів

Контрольні заходи включають у себе поточний та підсумковий контроль.

### **Поточний контроль.**

До форм поточного контролю належить оцінювання:

- рівня знань під час семінарських, практичних, лабораторних занять;
- якості виконання індивідуальної та самостійної роботи.

Поточний контроль здійснюється під час проведення семінарських, практичних та лабораторних занять і має за мету перевірку засвоєння знань, умінь і навичок курсантом (студентом, слухачем) з навчальної дисципліни.

У ході поточного контролю проводиться систематичний вимір приросту знань, їх корекція. Результати поточного контролю заносяться викладачем до журналів обліку роботи академічної групи за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»).

Оцінки за самостійну та індивідуальну роботи виставляються в журнали обліку роботи академічної групи окремою графою за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»). Результати цієї роботи враховуються під час виставлення підсумкових оцінок.

При розрахунку успішності здобувачів вищої освіти в Університеті враховуються такі види робіт: навчальні заняття (семінарські, практичні, лабораторні тощо); самостійна та індивідуальна роботи (виконання домашніх завдань, ведення конспектів першоджерел та робочих зошитів, виконання розрахункових завдань, підготовка рефератів, наукових робіт, публікацій, розроблення спеціальних технічних пристроїв і приладів, моделей, комп'ютерних програм, виступи на наукових конференціях, семінарах та інше); контрольні роботи (виконання тестів, контрольних робіт у вигляді, передбаченому в робочій програмі навчальної дисципліни). Вони оцінюються за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»).

**Результат навчальних занять за семестр** розраховується як середньоарифметичне значення з усіх виставлених оцінок під час навчальних занять протягом семестру та виставляється викладачем в журналі обліку роботи академічної групи окремою графою.

**Результат самостійної роботи за семестр** розраховується як середньоарифметичне значення з усіх виставлених оцінок з самостійної роботи, отриманих протягом семестру та виставляється викладачем в журналі обліку роботи академічної групи окремою графою.

**Курсант (студент, слухач), який отримав оцінку «незадовільно» за навчальні заняття або самостійну роботу, зобов'язаний перескласти її.**

Загальна кількість балів (оцінка), отримана здобувачем за семестр перед підсумковим контролем, розраховується як середньоарифметичне значення з оцінок за навчальні заняття та самостійну роботу, та для переводу до 100-бальної системи помножується на коефіцієнт **10**.

$$\text{Загальна кількість балів (перед підсумковим контролем)} = \left( \frac{\text{Результат навчальних занять за семестр} + \text{Результат самостійної роботи за семестр}}{2} \right) * 10$$

### **Підсумковий контроль.**

Підсумковий контроль проводиться з метою оцінки результатів навчання на певному ступені вищої освіти або на окремих його завершених етапах.

Для обліку результатів підсумкового контролю використовується поточно-накопичувальна інформація, яка реєструється в журналах обліку роботи академічної групи. Результати підсумкового контролю з дисциплін відображаються у відомостях обліку успішності, навчальних картках курсантів (студентів, слухачів), залікових книжках. **Присутність курсантів (студентів, слухачів) на проведенні підсумкового контролю (заліку, екзамену) обов'язкова.** Якщо курсант (студент, слухач) не з'явився на підсумковий контроль (залік, екзамен), то науково-педагогічний працівник ставить у відомість обліку успішності відмітку «не з'явився».

**Підсумковий контроль (екзамен, залік)** оцінюється за національною шкалою. Для переводу результатів, набраних на підсумковому контролі (екзамені, заліку), з національної системи оцінювання в 100-бальну вводиться коефіцієнт **10**, таким чином максимальна кількість балів на підсумковому контролі (екзамені, заліку), які використовуються при розрахунку успішності курсантів (студентів, слухачів), становить - **50**

Підсумкові бали з навчальної дисципліни визначаються як сума балів, отриманих здобувачем протягом семестру та балів, набраних на підсумковому контролі (екзамені, заліку).

$$\text{Підсумкові бали навчальної дисципліни} = \frac{\text{Загальна кількість балів (перед підсумковим контролем)}}{\text{підсумковим контролем}} + \frac{\text{Кількість балів за підсумковим контролем}}{\text{підсумковим контролем}}$$

Курсант (студент, слухач), який під час складання підсумкового контролю отримав оцінку «незадовільно», складає підсумковий контроль (екзамен, залік) повторно. Повторне складання підсумкового контролю (екзамену, заліку) допускається не більше двох разів з кожної навчальної дисципліни, у тому числі один раз – викладачеві, а другий – комісії, що створюється навчально-науковими інститутами (факультетами). Незадовільні оцінки виставляються тільки в відомостях обліку успішності. Курсантам (студентам, слухачам), які отримали не більше як дві незадовільні оцінки (нижче ніж 60 балів) з навчальної дисципліни, можуть бути встановлені різні строки ліквідації академічної заборгованості, але не пізніше як за день до фактичного початку навчальних занять у наступному семестрі. Курсанти (студенти, слухачі), які не ліквідували академічну заборгованість у встановлений термін, відраховуються з Університету. Особи, які одержали більше двох незадовільних оцінок (нижче ніж 60 балів) за підсумковими результатами вивчення навчальних дисциплін з урахуванням підсумкового контролю, відраховуються з Університету.

Якщо дисципліна вивчається протягом двох і більше семестрів з

семестровим контролем у формі підсумкового контролю (екзамену чи заліку), то результат вивчення дисципліни в поточному семестрі визначається як середньоарифметичне значення балів, набраних у поточному та попередньому семестрах.

$$\frac{\text{Підсумкові бали навчальної дисципліни}}{2} = \frac{\text{Підсумкові бали за поточний семестр}}{1} + \frac{\text{Підсумкові бали за попередній семестр}}{1}$$

У цьому розділі також повинні бути розроблені чіткі критерії оцінювання результатів роботи здобувачів вищої освіти під час поточного контролю (роботу на семінарських, практичних, лабораторних й інших аудиторних заняттях, виконання самостійних навчальних та індивідуальних творчих завдань) та підсумкового контролю. Кафедра визначає вимоги до здобувачів вищої освіти щодо засвоєння змісту навчальної дисципліни, а саме: кількість оцінок, яку він повинен отримати під час аудиторної роботи, самостійної або індивідуальної роботи. Наприклад:

Робота під час навчальних занять	Самостійна та індивідуальна робота	Модульний контроль
Отримати не менше 4 позитивних оцінок	Підготувати реферат, підготувати конспект за темою самостійної роботи, вирішити практичне завдання тощо.	Отримати за модульний контроль не менше 30 балів

## 9. Шкала оцінювання: національна та ECTS

Оцінка в балах	Оцінка за національною шкалою	Оцінка за шкалою ECTS	
		Оцінка	Пояснення
90 – 100	Відмінно (“зараховано”)	A	„Відмінно” – теоретичний зміст курсу освоєний <b>цілком</b> , необхідні практичні навички роботи з освоєним матеріалом сформовані, <b>всі</b> навчальні завдання, які передбачені програмою навчання, <b>виконані</b> в повному обсязі, відмінна робота без помилок або з однією незначною помилкою.
82 – 89	Добре (“зараховано”)	B	„Дуже добре” – теоретичний зміст курсу освоєний <b>цілком</b> , необхідні практичні навички роботи з освоєним матеріалом <b>в основному</b> сформовані, <b>всі</b> навчальні завдання, які передбачені програмою навчання, <b>виконані</b> , якість виконання <b>більшості</b> з них оцінено числом балів, близьким до <b>максимального</b> , робота з двома-трьома незначними помилками.
75 – 81		C	„Добре” – теоретичний зміст курсу освоєний <b>цілком</b> , практичні навички роботи з освоєним матеріалом <b>в основному</b> сформовані, <b>всі</b> навчальні завдання, які передбачені програмою навчання, <b>виконані</b> , якість виконання <b>жодного</b> з них <b>не оцінено мінімальним</b> числом балів, деякі види завдань виконані з <b>помилками</b> , робота з декількома незначними помилками або з однією–двома значними помилками.

68–74	Задовільно ("зараховано")	D	„Задовільно” – теоретичний зміст курсу освоєний <b>неповністю</b> , але <b>прогалини не несуть істотного</b> характеру, необхідні практичні навички роботи з освоєним матеріалом <b>в основному сформовані</b> , <b>більшість</b> передбачених програмою навчання навчальних завдань <b>виконано</b> , деякі з виконаних завдань містять <b>помилки</b> , робота з трьома значними помилками.
60–67		E	„Достатньо” – теоретичний зміст курсу освоєний <b>частково</b> , деякі практичні навички роботи <b>не сформовані</b> , <b>частина</b> передбачених програмою навчання навчальних завдань <b>не виконана</b> , або якість виконання деяких з них оцінено числом балів, близьким до <b>мінімального</b> , робота, що задовольняє мінімуму критеріїв оцінки.
35–59	Незадовільно („не зараховано”)	FX	„Умовно незадовільно” – теоретичний зміст курсу освоєний <b>частково</b> , необхідні практичні навички роботи <b>не сформовані</b> , <b>більшість</b> передбачених програм навчання, навчальних завдань <b>не виконано</b> , або якість їхнього виконання оцінено числом балів, близьким до <b>мінімального</b> ; при <b>додатковій самостійній</b> роботі над матеріалом курсу <b>можливе підвищення якості</b> виконання навчальних завдань (з <b>можливістю повторного складання</b> ), робота, що потребує доробки
1–34		F	„Безумовно незадовільно” – теоретичний зміст курсу <b>не освоєно</b> , необхідні практичні навички роботи <b>не сформовані</b> , <b>всі виконані</b> навчальні завдання містять <b>грубі помилки</b> , <b>додаткова самостійна</b> робота над матеріалом курсу <b>не приведе</b> до значимого <b>підвищення якості</b> виконання навчальних завдань, робота, що потребує повної переробки

## 10. Інформаційне та методичне забезпечення навчальної дисципліни

### 10.1. Рекомендована література

#### Основна література.

- Егоров, П.М. Метрология, стандартизация и сертификация в инфокоммуникациях: учеб. пособие для студ. Учреждений выс. Образования / П.М. Егоров – М.: Издательский центр «Академия», 2015.- 352с.
- Контрольно-измерительные приборы и инструменты : учеб. / С. А. Зайцев, Д. Д. Грибанов, А. Н. Толстов, Р. В. Меркулов. - М. : Академия, 2016.
- Участие в интеграции программных модулей : учеб. пособие / Г. Н. Федорова. - М. : Академия, 2016.
- Закон України “Про стандартизацію” від 05.06.2014 № 1315-VII
- Закон України „Про технічні регламенти та оцінку відповідності” від 15.01.2015 № 124-VIII
- Закон України “Про телекомунікації” від 18.11.2003 № 1280-IV (стаття 25)

7. Закон України “Про радіочастотний ресурс України” від 24.06.2004 № 1876-IV (стаття 27)
8. Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України, затверджено постановою Кабінету Міністрів України від 03.09.2014 № 411 (підпункти 40, 41, 45 пункту 4)
9. Положення про порядок розроблення, прийняття, перегляду і скасування галузевих нормативних документів зі стандартизації та галузевих будівельних норм, затверджено наказом Адміністрації Держспецзв’язку від 28.05.2012 № 262 (в редакції наказу Адміністрації Держспецзв’язку від 11.03.2015 № 123)
10. Конспект лекцій.

### **Додаткова література.**

1. Янчук В.О. Методика оцінювання стану захисту інформації локальних об’єктів системи електронного врядування. Ел. ресурс. Режим доступу : <http://academy.gov.ua/ej/ej11/txts/10ivoseu.pdf>
2. Велігура А.В. Оцінювання стану інформаційної безпеки підприємства. Ел. ресурс. Режим доступу : [www.irbis-nbuv.gov.ua/](http://www.irbis-nbuv.gov.ua/)
3. Сікорський Д.О. Аналіз принципів побудови моделей інформаційної безпеки в корпоративних інформаційних системах. Ел. ресурс. Режим доступу: <http://www.economy.nayka.com.ua/?op=1&z=4257>

### **ІНФОРМАЦІЙНІ РЕСУРСИ В ІНТЕРНЕТІ**

(перелік інформаційних ресурсів)

Тематичні бази даних [www.physics.vir.ru](http://www.physics.vir.ru), [ufn.ru/ru/articles/](http://ufn.ru/ru/articles/).  
Закордонні електронні наукові інформаційні ресурси: EuropeanLibrary. Вільний доступ до ресурсів 47 Національних бібліотек Європи, Австралії, Білорусії, Великої Британії, Німеччини, бібліотека коледжу Лондонського університету.  
<http://window.edu.ru/>  
[http://www.arcotel.ru/bibl/res\\_inet.php](http://www.arcotel.ru/bibl/res_inet.php)  
<http://www.ict.edu.ru/lib/index.php>  
<http://elibrary.rsl.ru/?menu=s410/elibrary/elibrary4454/science/&lang=ru>  
<http://dispace.edu.nstu.ru/didesk/index>